Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata

Nama Kelompok :

- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah

Tahapan 3: Simulasi brute force login (hydra / medusa)

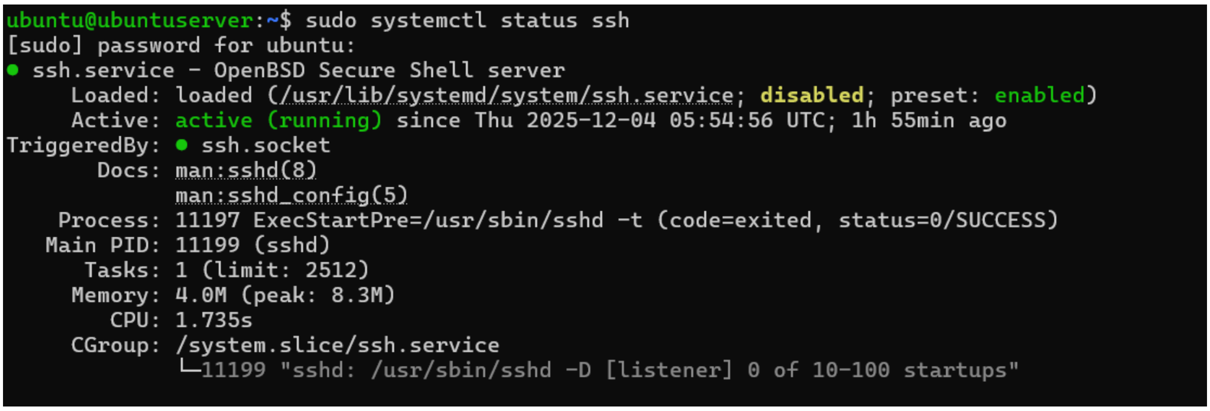
- Apa itu Brute force login (hydra / medusa)

Brute Force Login adalah teknik serangan siber yang mencoba mengakses sistem dengan cara mencoba banyak kemungkinan kombinasi username dan password secara sistematis hingga menemukan kredensial yang benar**.**

Hydra dan Medusa adalah alat otomatisasi untuk melakukan serangan brute force login terhadap berbagai protokol jaringan (SSH, FTP, HTTP, RDP, dll).

Proggres 1 - PERSIAPAN TARGET

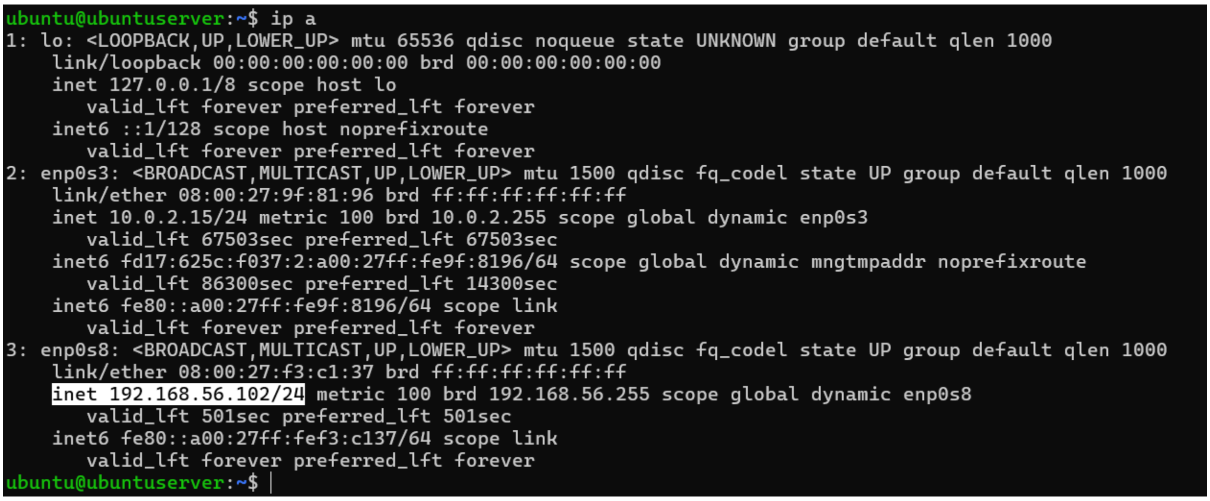
1. Memastikan SSH aktif (sudo systemctl status ssh)



```
ubuntu@ubuntuserver:~$ sudo systemctl status ssh
[sudo] password for ubuntu:
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: active (running) since Thu 2025-12-04 05:54:56 UTC; 1h 55min ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 11197 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 11199 (sshd)
      Tasks: 1 (limit: 2512)
     Memory: 4.0M (peak: 8.3M)
        CPU: 1.735s
     CGroup: /system.slice/ssh.service
             └─11199 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Dari gambar di atas jelas bahwa ssh sudah aktif (running)

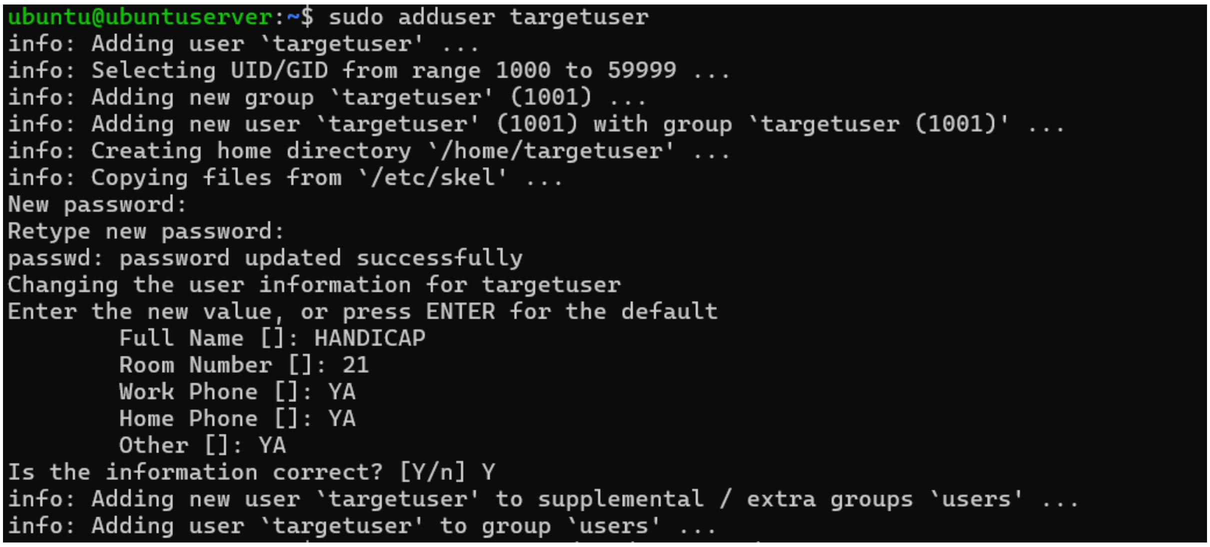
2. CEK IP ADDRESS UBUNTU (TARGET BRUTE FORCE) ip a



```
ubuntu@ubuntuserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9f:81:96 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 67503sec preferred_lft 67503sec
    inet6 fd17:625c:f037:2:a00:27ff:fe9f:8196/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86300sec preferred_lft 14300sec
    inet6 fe80::a00:27ff:fe9f:8196/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f3:c1:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 metric 100 brd 192.168.56.255 scope global dynamic enp0s8
       valid_lft 501sec preferred_lft 501sec
    inet6 fe80::a00:27ff:fef3:c137/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntuserver:~$ |
```

Ip target adalah 192,168.56.102

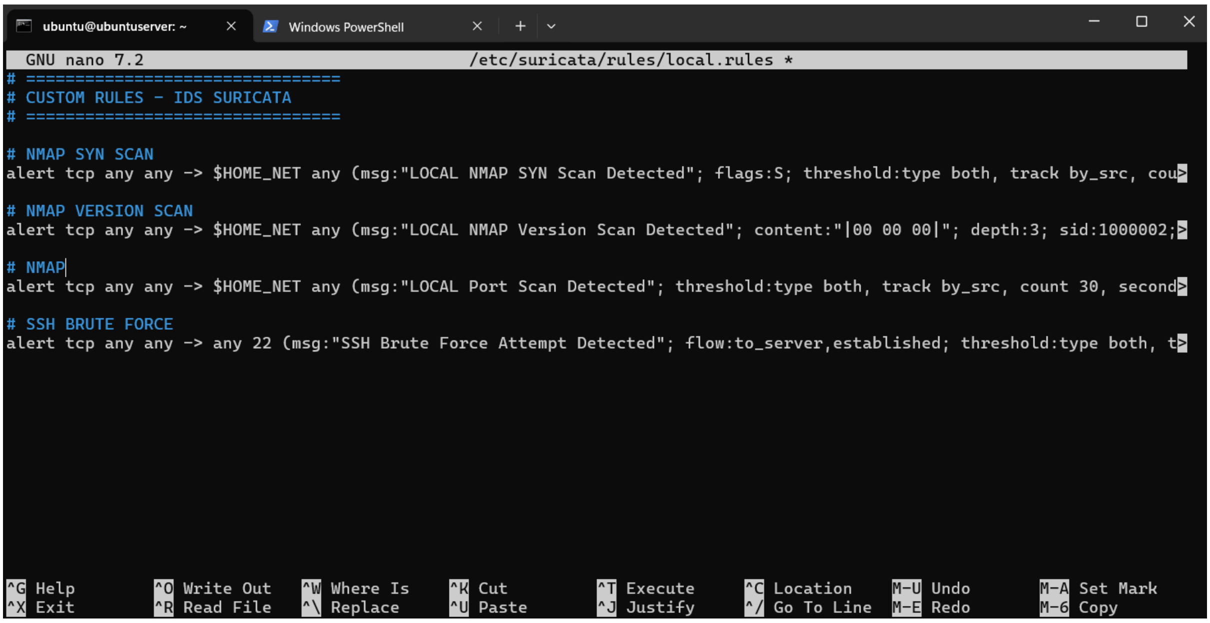
3. MEMBUAT USER TARGET UNTUK BRUTE FORCE



```
ubuntu@ubuntuserver:~$ sudo adduser targetuser
info: Adding user `targetuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `targetuser' (1001) ...
info: Adding new user `targetuser' (1001) with group `targetuser (1001)' ...
info: Creating home directory `/home/targetuser' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for targetuser
Enter the new value, or press ENTER for the default
        Full Name []: HANDICAP
        Room Number []: 21
        Work Phone []: YA
        Home Phone []: YA
        Other []: YA
Is the information correct? [Y/n] Y
info: Adding new user `targetuser' to supplemental / extra groups `users' ...
info: Adding user `targetuser' to group `users' ...
```

USER SUDAH DI BUAT DENGAN FULLNAME > HANDICAP

4. MEMBUAT RULE SURICATA UNTUK BRUTE FORCE SSH
    - sudo nano /etc/suricata/rules/local.rules

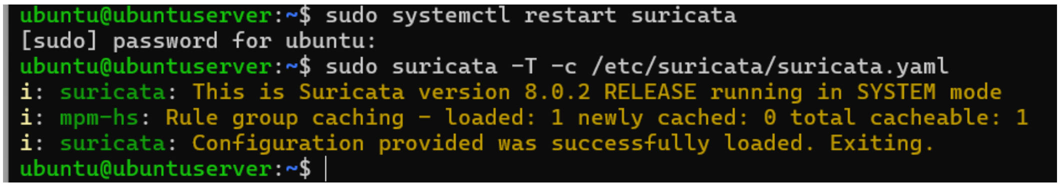


```
  GNU nano 7.2                               /etc/suricata/rules/local.rules *
# ================================
# CUSTOM RULES - IDS SURICATA
# ================================

# NMAP SYN SCAN
alert tcp any any -> $HOME_NET any (msg:"LOCAL NMAP SYN Scan Detected"; flags:S; threshold:type both, track by_src, cou>

# NMAP VERSION SCAN
alert tcp any any -> $HOME_NET any (msg:"LOCAL NMAP Version Scan Detected"; content:"|00 00 00|"; depth:3; sid:1000002;>

# NMAP
alert tcp any any -> $HOME_NET any (msg:"LOCAL Port Scan Detected"; threshold:type both, track by_src, count 30, second>

# SSH BRUTE FORCE
alert tcp any any -> any 22 (msg:"SSH Brute Force Attempt Detected"; flow:to_server,established; threshold:type both, t>









^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

Rules yang di tambahkan untuk ssh brute force :

alert tcp any any -> any 22 (msg:"SSH Brute Force Attempt Detected"; flow:to_server,established; threshold:type both, track by_src, count 5, seconds 60; sid:1000004; rev:1;)

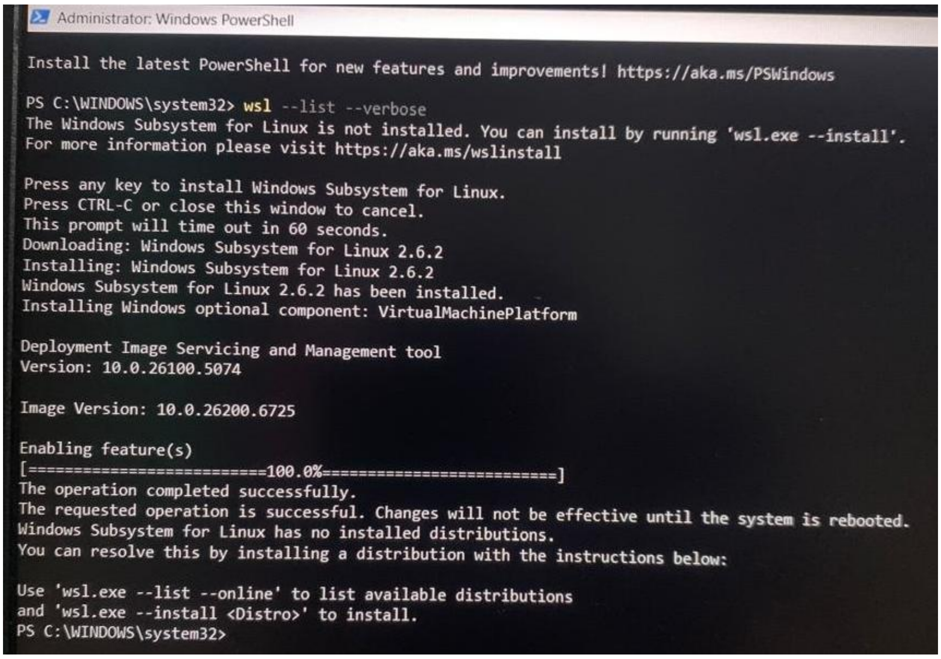
5. restart suricata dan cek eror rules



```
ubuntu@ubuntuserver:~$ sudo systemctl restart suricata
[sudo] password for ubuntu:
ubuntu@ubuntuserver:~$ sudo suricata -T -c /etc/suricata/suricata.yaml
i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
i: mpm-hs: Rule group caching - loaded: 1 newly cached: 0 total cacheable: 1
i: suricata: Configuration provided was successfully loaded. Exiting.
ubuntu@ubuntuserver:~$ |
```

Proggres 2 – Persiapan Attacker

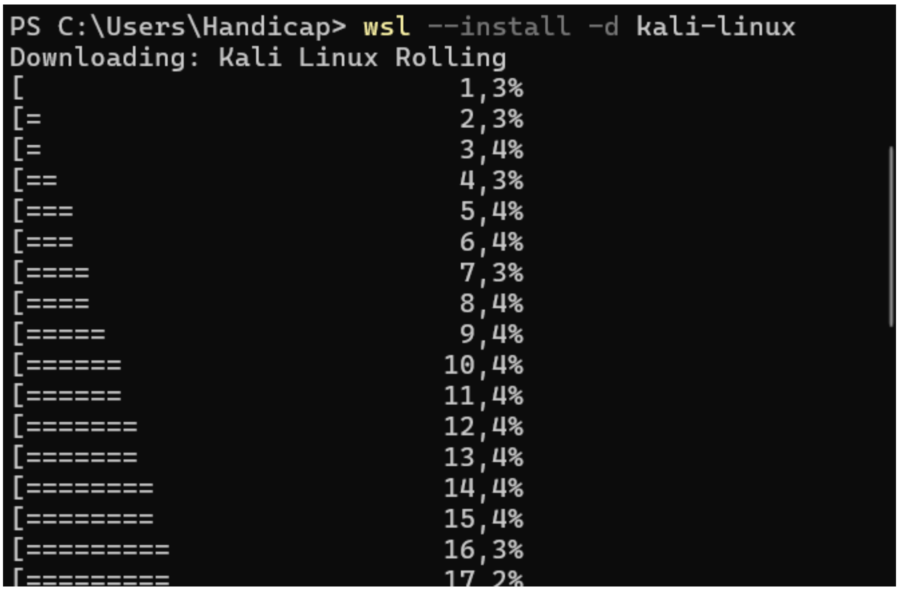
1. Hydra via WSL Kali Linux di Windows (cek dan instal wsl powershel as Administrator , wsl --list –verbose)



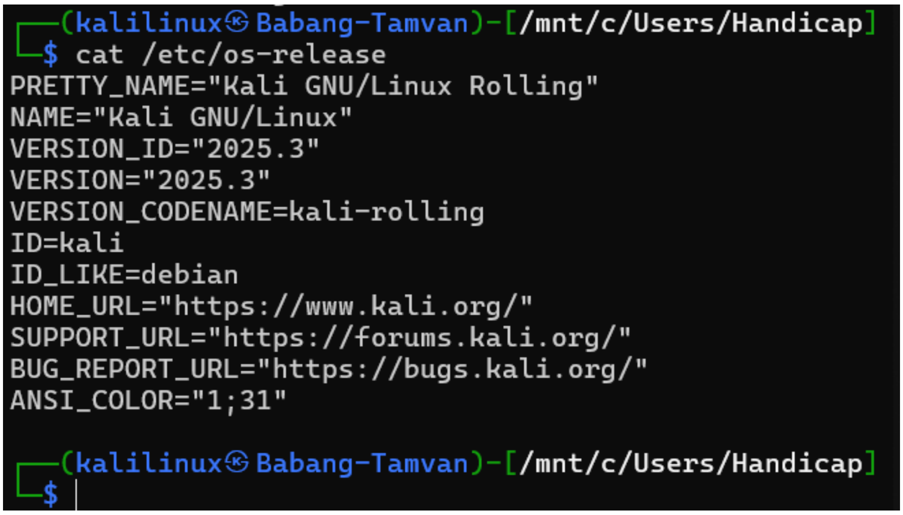
```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> wsl --list --verbose
The Windows Subsystem for Linux is not installed. You can install by running 'wsl.exe --install'.
For more information please visit https://aka.ms/wslinstall

Press any key to install Windows Subsystem for Linux.
Press CTRL-C or close this window to cancel.
This prompt will time out in 60 seconds.
Downloading: Windows Subsystem for Linux 2.6.2
Installing: Windows Subsystem for Linux 2.6.2
Windows Subsystem for Linux 2.6.2 has been installed.
Installing Windows optional component: VirtualMachinePlatform

Deployment Image Servicing and Management tool
Version: 10.0.26100.5074

Image Version: 10.0.26200.6725

Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.
The requested operation is successful. Changes will not be effective until the system is rebooted.
Windows Subsystem for Linux has no installed distributions.
You can resolve this by installing a distribution with the instructions below:

Use 'wsl.exe --list --online' to list available distributions
and 'wsl.exe --install <Distro>' to install.
PS C:\WINDOWS\system32>
```

Setelah di install lakukan restart windows

2. Instal kali linux dengan wsl

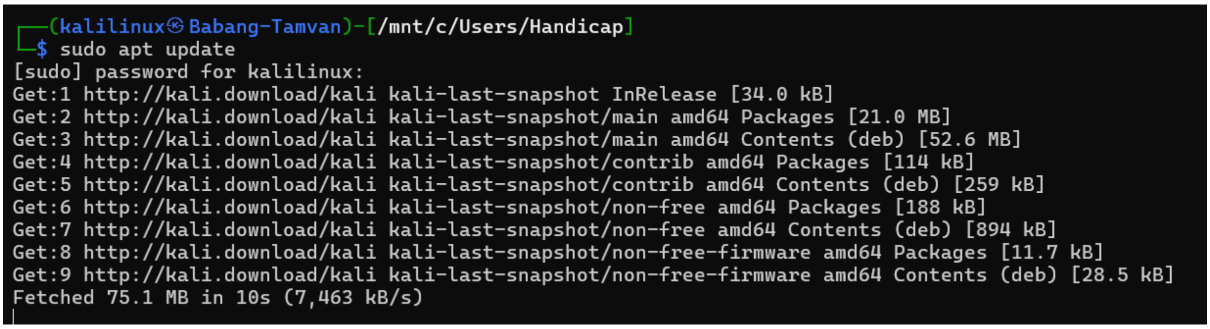


```
PS C:\Users\Handicap> wsl --install -d kali-linux
Downloading: Kali Linux Rolling
[                           1,3%
[=                          2,3%
[=                          3,4%
[==                         4,3%
[===                        5,4%
[===                        6,4%
[====                       7,3%
[====                       8,4%
[=====                      9,4%
[======                    10,4%
[======                    11,4%
[=======                   12,4%
[=======                   13,4%
[========                  14,4%
[========                  15,4%
[=========                 16,3%
[=========                 17,2%
```



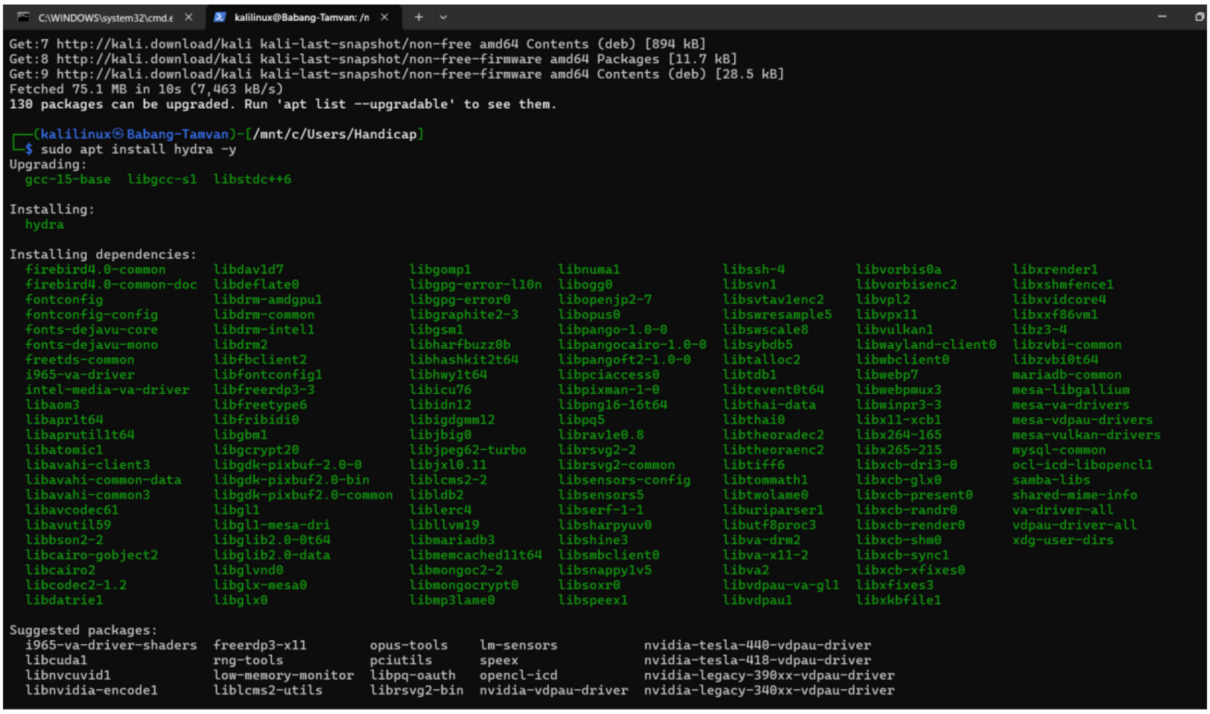
```
┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2025.3"
VERSION="2025.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"

┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ |
```

3. Lakukan update (sudo apt update)



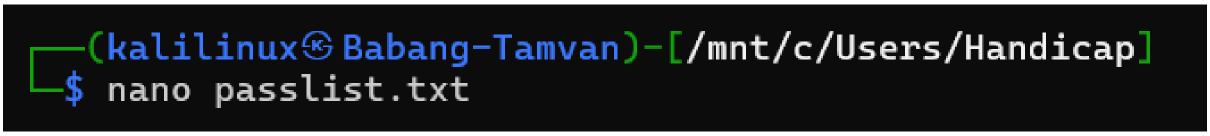
```
┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ sudo apt update
[sudo] password for kalilinux:
Get:1 http://kali.download/kali kali-last-snapshot InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-last-snapshot/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-last-snapshot/main amd64 Contents (deb) [52.6 MB]
Get:4 http://kali.download/kali kali-last-snapshot/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-last-snapshot/contrib amd64 Contents (deb) [259 kB]
Get:6 http://kali.download/kali kali-last-snapshot/non-free amd64 Packages [188 kB]
Get:7 http://kali.download/kali kali-last-snapshot/non-free amd64 Contents (deb) [894 kB]
Get:8 http://kali.download/kali kali-last-snapshot/non-free-firmware amd64 Packages [11.7 kB]
Get:9 http://kali.download/kali kali-last-snapshot/non-free-firmware amd64 Contents (deb) [28.5 kB]
Fetched 75.1 MB in 10s (7,463 kB/s)
|
```

4. Install hydra (sudo apt install hydra -y)



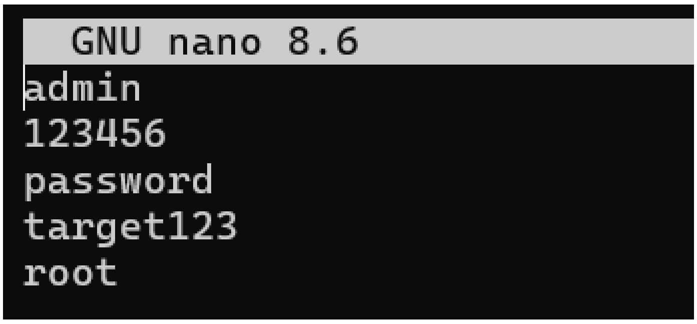
```
Get:7 http://kali.download/kali kali-last-snapshot/non-free amd64 Contents (deb) [894 kB]
Get:8 http://kali.download/kali kali-last-snapshot/non-free-firmware amd64 Packages [11.7 kB]
Get:9 http://kali.download/kali kali-last-snapshot/non-free-firmware amd64 Contents (deb) [28.5 kB]
Fetched 75.1 MB in 10s (7,463 kB/s)
130 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ sudo apt install hydra -y
Upgrading:
  gcc-15-base  libgcc-s1  libstdc++6

Installing:
  hydra

Installing dependencies:
  firebird4.0-common     libdav1d7               libgomp1          libnuma1            libssh-4        libvorbis0a        libxrender1
  firebird4.0-common-doc libdeflate0             libgpg-error-l10n libogg0             libsvn1         libvorbisenc2      libxshmfence1
  fontconfig             libdrm-amdgpu1          libgpg-error0     libopenjp2-7        libsvtav1enc2   libvpl2            libxvidcore4
  fontconfig-config      libdrm-common           libgraphite2-3    libopus0            libswresample5  libvpx11           libxxf86vm1
  fonts-dejavu-core      libdrm-intel1           libgsm1           libpango-1.0-0      libswscale8     libvulkan1         libz3-4
  fonts-dejavu-mono      libdrm2                 libharfbuzz0b     libpangocairo-1.0-0 libsybdb5       libwayland-client0 libzvbi-common
  freetds-common         libfbclient2            libhashkit2t64    libpangoft2-1.0-0   libtalloc2      libwbclient0       libzvbi0t64
  i965-va-driver         libfontconfig1          libhwy1t64        libpciaccess0       libtdb1         libwebp7           mariadb-common
  intel-media-va-driver  libfreerdp3-3           libicu76          libpixman-1-0       libtevent0t64   libwebpmux3        mesa-libgallium
  libaom3                libfreetype6            libidn12          libpng16-16t64      libthai-data    libwinpr3-3        mesa-va-drivers
  libapr1t64             libfribidi0             libigdgmm12       libpq5              libthai0        libx11-xcb1        mesa-vdpau-drivers
  libaprutil1t64         libgbm1                 libjbig0          librav1e0.8         libtheoradec2   libx264-165        mesa-vulkan-drivers
  libatomic1             libgcrypt20             libjpeg62-turbo   librsvg2-2          libtheoraenc2   libx265-215        mysql-common
  libavahi-client3       libgdk-pixbuf-2.0-0     libjxl0.11        librsvg2-common     libtiff6        libxcb-dri3-0      ocl-icd-libopencl1
  libavahi-common-data   libgdk-pixbuf2.0-bin    liblcms2-2        libsensors-config   libtommath1     libxcb-glx0        samba-libs
  libavahi-common3       libgdk-pixbuf2.0-common libldb2           libsensors5         libtwolame0     libxcb-present0    shared-mime-info
  libavcodec61           libgl1                  liblerc4          libserf-1-1         liburiparser1   libxcb-randr0      va-driver-all
  libavutil59            libgl1-mesa-dri         libllvm19         libsharpyuv0        libutf8proc3    libxcb-render0     vdpau-driver-all
  libbson2-2             libglib2.0-0t64         libmariadb3       libshine3           libva-drm2      libxcb-shm0        xdg-user-dirs
  libcairo-gobject2      libglib2.0-data         libmemcached11t64 libsmbclient0       libva-x11-2     libxcb-sync1
  libcairo2              libglvnd0               libmongoc2-2      libsnappy1v5        libva2          libxcb-xfixes0
  libcodec2-1.2          libglx-mesa0            libmongocrypt0    libsoxr0            libvdpau-va-gl1 libxfixes3
  libdatrie1             libglx0                 libmp3lame0       libspeex1           libvdpau1       libxkbfile1

Suggested packages:
  i965-va-driver-shaders freerdp3-x11       opus-tools   lm-sensors           nvidia-tesla-440-vdpau-driver
  libcuda1               rng-tools          pciutils     speex                nvidia-tesla-418-vdpau-driver
  libnvcuvid1            low-memory-monitor libpq-oauth  opencl-icd           nvidia-legacy-390xx-vdpau-driver
  libnvidia-encode1      liblcms2-utils     librsvg2-bin nvidia-vdpau-driver  nvidia-legacy-340xx-vdpau-driver
```

5. Pembuatan Daftar Password (Wordlist)



```
┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ nano passlist.txt
```

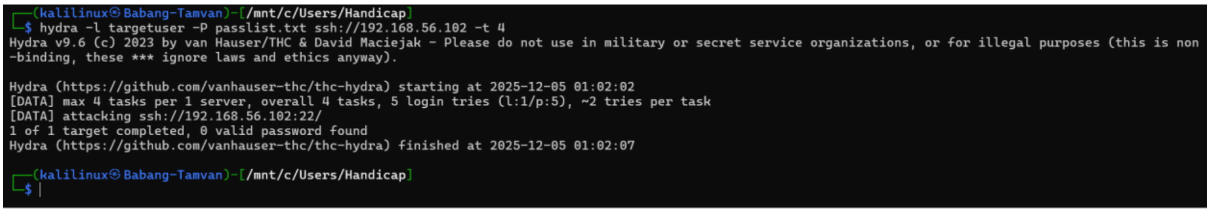
Isi dari file passlist.txt adalah sebagai berikut:



```
  GNU nano 8.6
admin
123456
password
target123
root
```

File ini berisi lima password umum yang sering digunakan pengguna, yang akan diuji satu per satu oleh tools Hydra untuk mencoba masuk ke akun SSH target.

6. Perintah Brute Force yang Digunakan (hydra -l targetuser -P passlist.txt ssh://192.168.56.102 -t 4)



```
┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ hydra -l targetuser -P passlist.txt ssh://192.168.56.102 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-05 01:02:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l:1/p:5), ~2 tries per task
[DATA] attacking ssh://192.168.56.102:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-05 01:02:07

┌──(kalilinux㉿Babang-Tamvan)-[/mnt/c/Users/Handicap]
└─$ |
```

Bagian Perintah	**Fungsi**
hydra	Menjalankan tools Hydra
-l targetuser	Username yang diserang
-P passlist.txt	Menggunakan file wordlist
ssh://192.168.56.102	Target SSH server
-t 4	Menjalankan 4 percobaan paralel

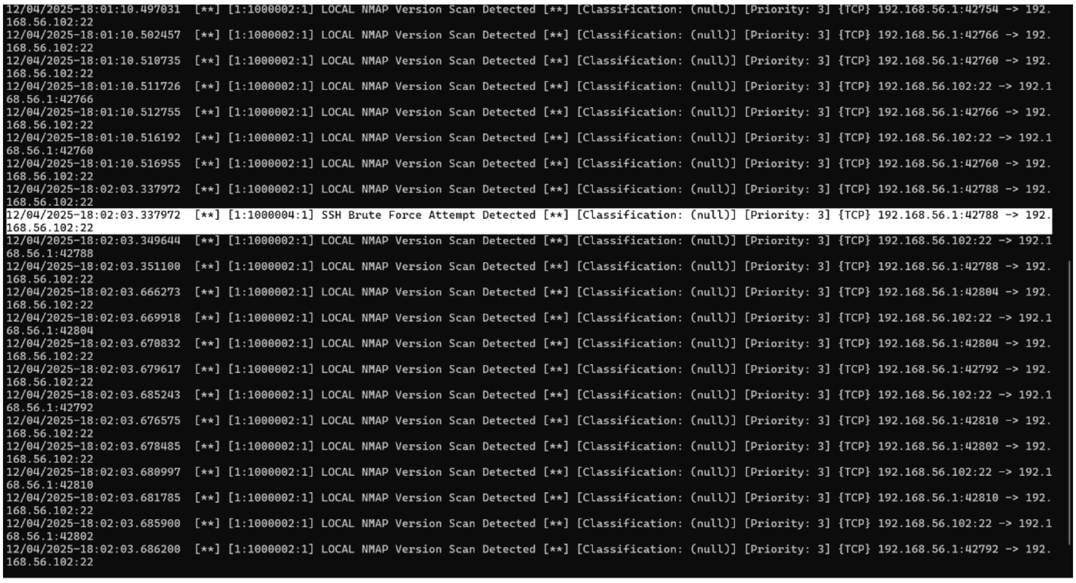
7. Hasil Eksekusi Hydra
   - ○ **1 of 1 target completed, 0 valid password found**

Artinya:

- Semua password dalam file wordlist sudah dicoba
- Tidak ada password yang berhasil
- Akun SSH target tidak berhasil ditembus
- Sistem SSH pada server dalam kondisi aman

8. Kesimpulan dari serangan
   Percobaan brute force menggunakan Hydra dengan wordlist buatan passlist.txt berhasil dijalankan terhadap layanan SSH pada server target. Meskipun tidak ditemukan password yang valid, sistem IDS Suricata tetap mampu mendeteksi aktivitas serangan dan menghasilkan alert SSH brute force. Hal ini menunjukkan bahwa IDS berfungsi dengan baik dalam memonitor dan mendeteksi ancaman jaringan.

9. Hasil Log Deteksi IDS Suricata



```
12/04/2025-18:01:10.497031  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42754 -> 192.
168.56.102:22
12/04/2025-18:01:10.502457  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42766 -> 192.
168.56.102:22
12/04/2025-18:01:10.510735  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42760 -> 192.
168.56.102:22
12/04/2025-18:01:10.511726  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42766
12/04/2025-18:01:10.512755  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42766 -> 192.
168.56.102:22
12/04/2025-18:01:10.516192  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42760
12/04/2025-18:01:10.516955  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42760 -> 192.
168.56.102:22
12/04/2025-18:02:03.337972  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42788 -> 192.
168.56.102:22
12/04/2025-18:02:03.337972  [**] [1:1000004:1] SSH Brute Force Attempt Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42788 -> 192.
168.56.102:22
12/04/2025-18:02:03.349644  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42788
12/04/2025-18:02:03.351100  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42788 -> 192.
168.56.102:22
12/04/2025-18:02:03.666273  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42804 -> 192.
168.56.102:22
12/04/2025-18:02:03.669918  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42804
12/04/2025-18:02:03.670832  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42804 -> 192.
168.56.102:22
12/04/2025-18:02:03.679617  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42792 -> 192.
168.56.102:22
12/04/2025-18:02:03.685243  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42792
12/04/2025-18:02:03.676575  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42810 -> 192.
168.56.102:22
12/04/2025-18:02:03.678485  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42802 -> 192.
168.56.102:22
12/04/2025-18:02:03.680997  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42810
12/04/2025-18:02:03.681785  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42810 -> 192.
168.56.102:22
12/04/2025-18:02:03.685900  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.102:22 -> 192.1
68.56.1:42802
12/04/2025-18:02:03.686200  [**] [1:1000002:1] LOCAL NMAP Version Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.56.1:42792 -> 192.
168.56.102:22
```

   ([1:1000004:1] SSH Brute Force Attempt Detected {TCP} 192.168.56.1:42788 -> 192.168.56.102:22)

   Suricata berhasil mendeteksi adanya percobaan login SSH berulang ke server target dari mesin attacker.

10. Kenapa log ssh brute force hanya 1 kali
    Rule yang di pakai yaitu (threshold: type both, track by_src, count 5, seconds 60;)
    Artinya:
    - Minimal 5 percobaan login dalam 60 detik
    - Baru 1 alert akan dicatat
    - Setelah itu alert tidak diulang sampai window waktu selesai
11. Kesimpulan Analisis Log
    Berdasarkan hasil pengujian, IDS Suricata berhasil mendeteksi aktivitas brute force SSH yang dilakukan menggunakan tools Hydra dari mesin attacker. Meskipun percobaan login dilakukan beberapa kali menggunakan beberapa password dalam wordlist, sistem hanya mencatat satu alert utama karena rule telah dikonfigurasi menggunakan mekanisme threshold untuk mencegah terjadinya alert flooding. Selain itu, muncul juga beberapa alert deteksi NMAP akibat karakteristik koneksi Hydra yang menyerupai aktivitas scanning. Hal ini menunjukkan bahwa IDS Suricata bekerja sesuai dengan pola deteksi yang telah dikonfigurasikan.